(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 18 209 A 1**

(51) Int. Cl.[7]: G 06 F 12/14

(21) Aktenzeichen: 101 18 209.0
(22) Anmeldetag: 11. 4. 2001
(43) Offenlegungstag: 24. 10. 2002

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Junk, Matthias, 86157 Augsburg, DE

(56) Entgegenhaltungen:
DE 196 20 346 A1
US 61 18 872

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Eingabeverfahren zur Authentifizierung

(57) Die Erfindung betrifft ein Verfahren zur Eingabe eines Authentifizierungscodes. Erfindungsgemäß wird auf einer Anzeigeeinrichtung eine Sequenz aus mehreren Bildern dargestellt, wobei jedes der Bilder während einer begrenzten Anzeigedauer dargestellt wird, den Bildern oder Bildteilen jeweils ein Code zugeordnet ist, und aus dem Code und/oder einem Zeitwert der Authentifizierungscode berechnet wird.

DE 101 18 209 A 1

DE 101 18 209 A 1

BNSDOCID: <DE 10118209A1 | >

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Eingabe eines Authentifizierungscodes.

[0002] Ein solcher Authentifizierungscode ist beispielsweise ein Passwort oder eine persönliche Identifizierungsnummer (PIN). Ein solcher Code wird im Allgemeinen über eine Tastatur eingegeben.

[0003] Probleme bei dieser Methode sind zum Einen das unbeobachtete Eingeben des Codes und zum Anderen das Merken desselben.

[0004] Der Erfindung liegt die Aufgabe zugrunde, ein einfaches und sicheres Eingabeverfahren für einen Authentifizierungscode anzugeben.

[0005] Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch angegebenen Merkmale gelöst.

[0006] Im Folgenden wird die Erfindung anhand eines Ausführungsbeispieles beschrieben.

[0007] Das erfindungsgemäße Eingabeverfahren ermöglicht eine kreative und personalisierbare Zugangssicherung.

[0008] Die Erfindung geht aus von einem visuellen Eingabemechanismus. Bei diesem werden die alphanumerischen Zeichen des Authentifizierungscodes durch Bilder ersetzt. Auf dem Bildschirm werden beispielsweise zehn Bilder dargestellt, wobei jedem der Bilder ein Buchstabe beziehungsweise eine Ziffer zugeordnet ist. Der Benutzer weiss welche Bilder er in welcher Reihenfolge anklicken muss, um so den entsprechenden Code einzugeben. Der Benutzer kann hierzu persönliche Bilder verwenden, was die Merkbarkeit erleichtert.

[0009] Erfindungsgemäß wird eine Bildsequenz, das heisst eine Aufeinanderfolge von Bildern auf der Anzeigeeinrichtung dargestellt. Auch hier ist wieder jedem der Bilder ein alphanumerisches Zeichen zugeordnet. Es kann dabei ein Videofilm verwendet werden, oder auch im einfachsten Fall eine Folge von unabhängigen Standbildern. Jedes der Bilder erscheint beispielsweise für eine Sekunde, und kann während dieser Zeitspanne durch Anklicken ausgewählt werden. Durch die Auswahl wird das diesem Bild zugeordnete Zeichen für die Eingabe des Authentifizierungscodes aktiviert.

[0010] Bei einer Weiterbildung der Erfindung ist nur ein Bildteil aktivierbar. Dieser Teil ist beispielsweise durch seine Koordinaten gegeben, die einen Code darstellen. Dieser Code wird, bei einer weiter Ausgestaltung der Erfindung zusammen mit einem Zeitwert, bei einer Berechnung des Authentifizierungscodes verwendet. Der Zeitwert kann durch die Anzeigedauer des betreffenden Bildes gegeben sein.

[0011] Weiter kann bei der Berechnung des Authentifizierungscodes noch ein Verschlüsselungsalgorithmus eingesetzt werden.

[0012] Durch die zeitliche Einschränkung wird die Sicherheit bei der Codeeingabe erhöht.

Patentansprüche

Verfahren zur Eingabe eines Authentifizierungscodes, **dadurch gekennzeichnet**, dass auf einer Anzeigeeinrichtung eine Sequenz aus mehreren Bildern dargestellt wird, wobei jedes der Bilder während einer begrenzten Anzeigedauer dargestellt wird, den Bildern oder Bildteilen jeweils ein Code zugeordnet ist, und aus dem Code und/oder einem Zeitwert der Authentifizierungscode berechnet wird.

2334a IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences
E78-A(1995) May, No. 5, Tokyo, JP

p. 577-578 = (2)

LETTER *Special Section of Letters Selected from the 1994 IEICE Fall Conference*

Evaluating Security of a Simple Interactive Human Identification Scheme*

Ryo MIZUTANI† *and* Tsutomu MATSUMOTO†, *Members*

SUMMARY Password checking schemes are human identification methods commonly adopted in many information systems. One of their disadvantages is that an attacker who correctly observed an input password can impersonate the corresponding user freely. To overcome it there have been proposed interactive human identification schemes. Namely, a human prover who has a secret key is asked a question by a machine verifier, who then checks if an answer from the prover matches the question with respect to the key. This letter examines such a scheme that requires relatively less efforts to human provers. By computer experiments this letter evaluates its resistance against a type of attack; after observing several pairs of questions and correct answers how successfully can an attacker answer the next question?

key words: authentication, human cryptography, human interface, identification, information security, passwords

1. Introduction

Figure 1 illustrates the above mentioned difference between conventional password schemes and interactive human identification schemes firstly examined in Ref. [1]. A brief description on the feature and the significance of the latter class by contrast with schemes requiring auxiliary devices for provers can be also found in Ref. [1]. A simple interactive identification scheme [2] is easy to understand and requiring no randomness to make an answer. However its security is not clearly developed in Ref. [2]. It is thus interesting to investigate if the scheme achieves acceptable security level with moderate sizes of parameters. This letter experimentally clarifies the resistance of the scheme against a scenario of attack.

2. The Scheme

Definition 1: For positive integers s and t, let Ω be a set of $s \cdot t$ elements. An *ordered uniform s-partition* of Ω is defined by

$$Q = \{(j, Q_j) \mid Q_j \subset \Omega: \bigcup_{j=1}^{s} Q_j = \Omega; \#Q_j = t: \quad j = 1, 2, \cdots, s\}.$$

For (j, Q_j), Q_j is called the *j-th cell* of Q and j is called the *cell id* of cell Q_j. Let $\mathcal{Q}_{(s,t)}(\Omega)$ denote the set of all ordered uniform s-partitions of Ω.

Now we formally define the scheme as a protocol conducted by two players, *Prover* and *Verifier*.

Definition 2: Scheme D

Preparation Phase

0. *Prover* and *Verifier* agree on positive integers s, t, u, set Ω of $s \cdot t$ elements, and $k = [k_1, k_2, \cdots, k_u]$, called a *key*, randomly and uniformly selected from Ω^u. *Prover* and *Verifier* keep k secret.

Execution Phase

1. *Verifier* selects an ordered uniform s-partition, Q, called a *question*, randomly and uniformly from $\mathcal{Q}_{(s,t)}(\Omega)$, and displays Q.
2. Given $Q = \{(j, Q_j) \mid j = 1, 2, \cdots, s\}$, *Prover* composes an *answer*,

$$a = \{(i, a_i) \mid k_i \in Q_{a_i};\ i = 1, 2, \ldots, u\},$$

using k, and inputs a to *Verifier*. In other words, for each $i = 1, 2, \ldots, u$, *Prover* finds the cell containing k_i, and puts its cell id as a_i.
3. *Verifier* checks whether a matches Q with respect to k, namely, $k_i \in Q_{a_i}$ for every $i = 1, 2, \cdots, u$, *Verifier* accepts *Prover* if and only if a matches Q.

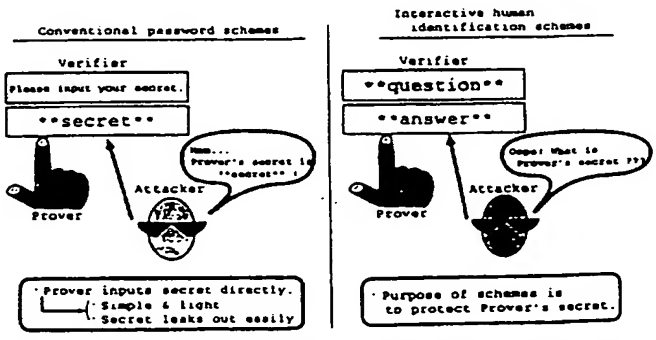

Fig. 1 Conventional password schemes & interactive human identification schemes.

Manuscript received October 23, 1994.
Manuscript revised December 22, 1994.

†The authors are with the Division of Electrical and Computer Engineering, Yokohama National University, Yokohama-shi, 240 Japan.

*A preliminary version of this work was presented at the 1994 IEICE Fall Conference: Presentation A-190.

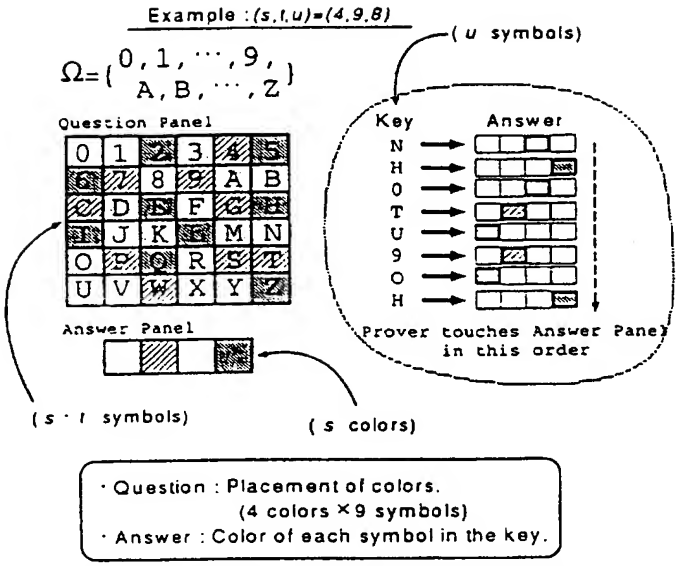

Fig. 2 A graphical implementation of Scheme D.

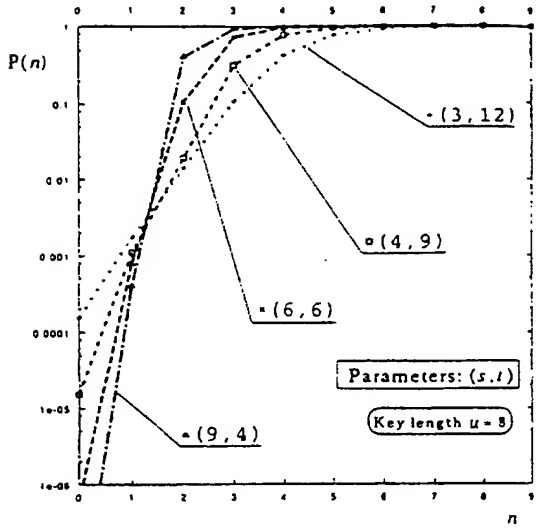

Fig. 3 Success rate P(n) vs. number of pairs n.

Figure 2 shows a graphical implementation of Scheme D,where parameters (s,t,u) are $(4,9,8)$, $\Omega = \{0,\cdots,9,A,\cdots,Z\}$, and $k = [N,H,0,T,U,9,O,H]$; Colors in Answer Panel correspond to cell ids 1, 2, 3, 4, from the left to the right.

3. The Attack

When the third player, *Attacker*, cannot peep questions and answers, he can make a correct answer that matches a newly given question with probability $1/s^u$.

Next, assume *Attacker* can peep pairs of questions and correct answers transferred in n (≥ 1) rounds of executions. For $r = 1,\cdots,n$, let $Q^{(r)} = \{(j, Q_j^{(r)}) \mid j = 1,2,\cdots,s\}$ and $a^{(r)} = \{(i, a_i^{(r)}) \mid i = 1,2,\ldots,u\}$ be the pair observed in the r-th round. Using these data *Attacker* tries to make a correct answer that matches a newly given question.

Definition 3: Attack
For $n \geq 1$ *Attacker* computes the set of candidate keys:

$$K_i^{(n)} = \bigcap_{r=1}^{n} Q^{(r)}_{a_i^{(r)}}, \quad i = 1,\cdots,u.$$

Given question Q, for $i = 1,\cdots,u$, *Attacker* finds $\tilde{a}_i$ that is any integer j $(= 1,\cdots,s)$ maximizing $\#(K_i^{(n)} \cap Q_j)$. Then *Attacker* sends to *Verifier*

$$\tilde{a} = \{(i,\tilde{a}_i) \mid i = 1,2,\cdots,u\}$$

as the candidate answer to Q.

It is easy to see that $k_i \in K_i^{(n)}$ for $i = 1,\cdots,u$.

4. Experimental Result and Discussion

We conducted a computer experiment for $u = 8$ and $(s,t) = (3,12),(4,9),(6,6),(9,4)$, namely $s \cdot t = 36$. These parameters fit the practical implementation where relatively tractable eight alphanumeric characters can be used as a key. For each $n(=1,2,\cdots,9)$, the experiment attacked the scheme 10^5 times. Figure 3 plots the success rate $P(n)$. $P(0)$ is set as $1/s^u$.

The described attack seems powerful but not optimal since it doesn't utilize the information obtained by unsuccessful answering. Figure 3 tells that the success rate $P(n)$ for Scheme D is not equal to 1 with small values of n. If a bigger u is adopted a smaller $P(n)$ can be achieved but larger capacity may be required to memorize a key. In contrast, the simple password scheme with a password $k \in \Omega$ has the profile that when $n = 0$ the success rate is $1/(s \cdot t)^u \ll 1/s^u$ but it is 1 for any positive n.

Remaining research subjects include: Evaluating the security of Scheme D under the condition that *Attacker* can impersonate *Verifier* and choose questions; Constructing practical interactive human identification schemes stronger than Scheme D in a way that their resistance can be formally assured.

References

[1] Matsumoto, T. and Imai, H., "Human identification through insecure channel," *Advances in Cryptology – EUROCRYPT '91, LNCS* 547, pp.409–421, Springer-Verlag, 1991.
[2] Ijima, H. and Matsumoto, T., "A simple scheme for challenge-response type human identification," *in Proc. of Symposium on Cryptography and Information Security, IEICE, SCIS94-13C*, Jan. 1994.